



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/518,415	08/16/2005	Carlo Antonio Giovanni D'Agnolo	72998-012200	9943
7590		08/01/2008		
Charles Berman Greenberg Traurig 2450 Colorado Avenue Suite 400E Santa Monica, CA 90404			EXAMINER	
			ABRISHAMKAR, KAVEH	
			ART UNIT	PAPER NUMBER
			2131	
MAIL DATE		DELIVERY MODE		
08/01/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/518,415 Examiner KAVEH ABRISHAMKAR	Applicant(s) D'AGNOLO, CARLO ANTONIO GIOVANNI Art Unit 2131
------------------------------	--	---

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 April 2008.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,2,4-6 and 8-12 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,2,4-6 and 8-12 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 4/8/08
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 8, 2008 has been entered.
2. Claims 1-2, 4-6, and 8-12 are currently being considered.

Response to Arguments

Applicant's arguments filed April 8, 2008 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA) does not teach reading machine readable holder details from a machine readable zone and checking the predetermined relationship of the data to the machine readable holder details. This argument is not found persuasive. Chen (U.S. Patent 5,694,471) was used to teach this element of the claims. Chen teaches a system wherein a card stores a checksum which is created by using a one-way hash of the user information and the issuer identification number (Chen: column 6, lines 47-55). This information is used to generate a PIN (Chen: column 6, lines 53-56). Then when the card is inserted into the

transaction processing terminal (TPT), a PIN is computed and compared to the PIN which is stored, and if the PINs match, the user is authenticated (Chen: column 10, lines 14-29). Therefore, the machine readable holder details is the PIN which was generated by using the user information, and checking the relationship would be comparing the PINs.

Regarding claim 1, the Applicant further argues that the CPA does not teach authenticating the biometric data stored in the chip. Burger discloses storing biometric data on a chip (Burger: column 5, lines 32-36). Trench discloses a private key which is used in challenge response to establish the authenticity of the chip (Trench: paragraph 0026, lines 10-11). The combination of Burger-Trench, therefore provides a card with a chip which stores a private key and biometric data. However, they do not teach verifying the authenticity of the data itself, but only the chip. However, Chen uses a system of using stored digital signatures to calculate a checksum, which was originally calculated using the user's information, and compares it to the stored checksum (Chen: column 9, line 55 – column 10, line 10). If the checksums (user information) do not match, then the card is rejected. The user information in this case could include the biometric information of Burger. It would have been obvious to combine Chen with the Burger-Trench combination because all three are directed towards authenticating users and chip cards.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-2, 5-12, and 15-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Burger (U.S. Patent 6,219,439) in view of Trench (U.S. Patent Publication No. US 2005/0154877 A1) in further in view of Chen et al. (U.S. Patent 5,694,471).

Regarding claim 1, Burger discloses:

System for reading a document comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has predetermined right, which document at least contains a chip contained one or more private keys and a biocertificate containing biometric data (column 5, lines 32-26: *user fingerprint information stored on chip*) on a holder as well as data with a predetermined relationship to the machine readable holder details in the machine readable zone, which predetermined relationship is based on a one-way function and wherein the system comprises:

a reader for reading the chip (Figure 1, item 12, column 6, lines 13-16: the reader “scans the user’s fingerprint and compares it against the stored template of the same print on the smart card”);

a memory containing details with regard to the predetermined right of the holder (column 5, lines 36-37: *identification data stored in chip memory*);

a biometric feature scanner arranged to scan a biometric feature of the holder and to generate scanned biometric data (Figure 1, item 16, column 5, lines 8-13: *"fingerprint scanner platen"*);

a processing unit that is connected to the reader, the memory and the biometric feature scanner (column 5, lines 50-58, column 6, lines 13-18: *authentication done on board reader*) and is equipped to:

receive the biometric data on the holder from the chip, from the reader (column 5, lines 34-37, column 6, lines 13-16: *the fingerprint data on the chip is read and compared to the input fingerprint*);

receive the biometric data on the person presenting the document from the biometric feature scanner (column 5, lines 50-51: *user places finger on fingerprint scanner*) and to compare these with the biometric data on the holder to determine whether the person presenting the document is the holder (column 5, lines 50-55: *compare input fingerprint with stored fingerprint data to determine if user is authentic*);

receive the holder details via the reader (column 5, lines 36-37: "identification data"), check the predetermined relationship between the holder details and the data (column 5, lines 50-55: *authenticating user*) and read the predetermined right of holder from the memory (column 6, lines 45-51: *wherein the user identification memory (predetermined right) is used to determine if the user is able to gain entry*);

provide a signal to indicate the predetermined right for the person presenting the document if the chip and the biocertificate are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder (column 7, lines 46-51), *wherein the response (signal) is sent to a gateway indicating whether access is permitted.*

Burger does not explicitly disclose that the processing unit establishes the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip and the data with the aid of a public key encryption technology. Trench discloses a system wherein a chip card contains a private key (Trench: Figure 2, item 104), which is used in a challenge along with a public key to determine if the chip card is authentic (Trench: paragraph 0026, lines 1-12). Burger and Trench are analogous arts as both use chip cards to authenticate a user. Trench uses this challenge system to assure that the chip card is authentic before letting the user proceed with a transaction (Trench: paragraph 0026, lines 10-11). This challenge-response using the private-public key technology could be used in the system of Burger after the biometric input is compared to authenticate the user. In the system of Burger, after the authentication of the user, the user identification data is read from the chip and sent to a gateway (Burger: column 6, lines 44-51). The gateway could then send a challenge to the user to verify that the chip is also authentic, as in the system of Trench, which using the method of Trench, the user can use the stored

private key to respond to the challenge to verify that the chip is also authentic and allow the transaction to proceed (Trench: paragraph 0026: lines 1-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the public-private encryption method of Trench into the system of Burger so that a merchant "can be assured that the user is the legitimate certificate holder and that the user certificate belongs to the user" (Trench: paragraph 0026, lines 8-11) and so that the merchant can "confidently accept the chip card from the user" (Trench: paragraph 0026, lines 11-12).

Burger discloses storing biometric data on a chip (Burger: column 5, lines 32-36). Trench discloses a private key which is used in challenge response to establish the authenticity of the chip (Trench: paragraph 0026, lines 10-11). The combination of Burger-Trench, therefore provides a card with a chip which stores a private key and biometric data. However, they do not teach verifying the authenticity of the data itself, but only the chip. However, Chen uses a system of using stored digital signatures to calculate a checksum, which was originally calculated using the user's information, and compares it to the stored checksum (Chen: column 9, line 55 – column 10, line 10). If the checksums (user information) do not match, then the card is rejected. The user information in this case could include the biometric information of Burger. It would have been obvious to combine Chen with the Burger-Trench combination because all three are directed towards authenticating users and chip cards.

Burger and Trench do not explicitly teach reading the machine readable holder details from a machine readable zone and checking the predetermined relationship of

Art Unit: 2131

the data to the machine readable holder details. Chen discloses a system wherein a card stores issuer identification information (holder details) and a key which it uses to perform a one-way hash function on the user information data (Chen: column 6, lines 50-54, column 7, lines 57-63) and then the authentication unit performs its own checksum on the issuer identification number and compares the results to authenticate the user (Chen: column 7, lines 18-29). Burger discloses a key that is stored on the card, so this key can be used to perform the hash value on the user information to create a hash, which is then compared to a hash of the results at the gateway of Burger using the process of Chen (predetermined relationship to the holder details). Burger, Trench, and Chen are analogous arts as all use chip cards for the purposes of authenticating a user. It would have been obvious to use the one-way hashing function of Chen to authenticate the user information in the system of Burger-Trench because the use of a one-way function because it "makes it impossible to work backwards to determine the checksum" (Chen: column 4, lines 9-14).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Burger discloses:

System according to claim 1, wherein the document is a travel document (column 5, lines 43-46), *wherein the smart card (document) could operate as a driver's license.*

Claim 4 is rejected as applied above in claim 3. Furthermore, the system of Burger-Trench-Chen teaches that the one-way function is a hashing function (Chen: column 6,

lines 50-54), wherein a on-way hashing function is performed on the user identification information.

Regarding claim 5, Burger discloses:

Method for reading a document provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has a predetermined right, which document contains at least one chip containing one or more private keys and a biocertificate containing biometric data (column 5, lines 32-26: *user fingerprint information stored on chip*) on a holder as well as data having a predetermined relationship to the machine readable holder details, and wherein the system comprises a reader for reading the chip and for reading the machine-readable holder details (Figure 1, item 12, column 6, lines 13-16: the reader “scans the user's fingerprint and compares it against the stored template of the same print on the smart card”), a memory containing data on the predetermined right of the holder (column 5, lines 36-37: *identification data stored in chip memory*), a biometric feature scanner arranged to scan a biometric feature of the holder and to generate scanned biometric data (Figure 1, item 16, column 5, lines 8-13: “*fingerprint scanner platen*”) and a processing unit that is connected to the reader, the memory, and the biometric feature scanner (column 5, lines 50-58, column 6, lines 13-18: *authentication done on board reader*), wherein the method comprises the following operations:

receipt of the biometric data on the holder from the chip (column 5, lines 34-37, column 6, lines 13-16: *the fingerprint data on the chip is read and compared to the input fingerprint*);

receipt of the biometric data on the person presenting the document (column 5, lines 50-51: *user places finger on fingerprint scanner*) and comparison with the biometric data on the holder to determine whether the person presenting the document is the holder (column 5, lines 50-55: *compare input fingerprint with stored fingerprint data to determine if user is authentic*);

receipt of the holder details (column 5, lines 36-37: "identification data"), checking of the specific relationship between the holder details and the data (column 5, lines 50-55: *authenticating user*) and reading the predetermined right of the holder from the memory (column 6, lines 45-51: *wherein the user identification memory (predetermined right) is used to determine if the user is able to gain entry*);

provision of a signal to indicate the predetermined right for the person presenting the document if the chip and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder (column 7, lines 46-51), *wherein the response (signal) is sent to a gateway indicating whether access is permitted*.

Burger does not explicitly disclose that the processing unit establishes the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing

said random challenge code by said chip and the data with the aid of a public key encryption technology. Trench discloses a system wherein a chip card contains a private key (Trench: Figure 2, item 104), which is used in a challenge along with a public key to determine if the chip card is authentic (Trench: paragraph 0026, lines 1-12). Burger and Trench are analogous arts as both use chip cards to authenticate a user. Trench uses this challenge system to assure that the chip card is authentic before letting the user proceed with a transaction (Trench: paragraph 0026, lines 10-11). This challenge-response using the private-public key technology could be used in the system of Burger after the biometric input is compared to authenticate the user. In the system of Burger, after the authentication of the user, the user identification data is read from the chip and sent to a gateway (Burger: column 6, lines 44-51). The gateway could then send a challenge to the user to verify that the chip is also authentic, as in the system of Trench, which using the method of Trench, the user can use the stored private key to respond to the challenge to verify that the chip is also authentic and allow the transaction to proceed (Trench: paragraph 0026: lines 1-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the public-private encryption method of Trench into the system of Burger so that a merchant "can be assured that the user is the legitimate certificate holder and that the user certificate belongs to the user" (Trench: paragraph 0026, lines 8-11) and so that the merchant can "confidently accept the chip card from the user" (Trench: paragraph 0026, lines 11-12).

Burger discloses storing biometric data on a chip (Burger: column 5, lines 32-36). Trench discloses a private key which is used in challenge response to establish the authenticity of the chip (Trench: paragraph 0026, lines 10-11). The combination of Burger-Trench, therefore provides a card with a chip which stores a private key and biometric data. However, they do not teach verifying the authenticity of the data itself, but only the chip. However, Chen uses a system of using stored digital signatures to calculate a checksum, which was originally calculated using the user's information, and compares it to the stored checksum (Chen: column 9, line 55 – column 10, line 10). If the checksums (user information) do not match, then the card is rejected. The user information in this case could include the biometric information of Burger. It would have been obvious to combine Chen with the Burger-Trench combination because all three are directed towards authenticating users and chip cards.

Burger and Trench do not explicitly teach reading the machine readable holder details from a machine readable zone and checking the predetermined relationship of the data to the machine readable holder details. Chen discloses a system wherein a card stores issuer identification information (holder details) and a key which it uses to perform a one-way hash function on the user information data (Chen: column 6, lines 50-54, column 7, lines 57-63) and then the authentication unit performs its own checksum on the issuer identification number and compares the results to authenticate the user (Chen: column 7, lines 18-29). Burger discloses a key that is stored on the card, so this key can be used to perform the hash value on the user information to create a hash, which is then compared to a hash of the results at the gateway of Burger

using the process of Chen (predetermined relationship to the holder details). Burger, Trench, and Chen are analogous arts as all use chip cards for the purposes of authenticating a user. It would have been obvious to use the one-way hashing function of Chen to authenticate the user information in the system of Burger-Trench because the use of a one-way function because it "makes it impossible to work backwards to determine the checksum" (Chen: column 4, lines 9-14).

Regarding claim 6, Burger discloses:

Data carrier comprising a computer program that can be loaded by a system for reading a document comprising a card provided with machine-readable holder details in a machine-readable zone and for establishing whether a person presenting the document has a predetermined right, which document contains at least one chip containing a biometric data on a holder (column 5, lines 32-26: *user fingerprint information stored on chip*) as well as data having a predetermined relationship to the holder details, and wherein the system comprises a reader for reading the chip and the machine-readable holder details (Figure 1, item 12, column 6, lines 13-16: the reader "scans the user's fingerprint and compares it against the stored template of the same print on the smart card"), a memory containing data on the predetermined right of the holder (column 5, lines 36-37: *identification data stored in chip memory*), a biometric feature scanner and a processing unit that is connected to the reader, the memory and the biometric feature scanner (Figure 1, item 16, column 5, lines 8-13: "fingerprint

scanner platen"), wherein the computer program can provide the system with the following functionality:

receipt of the biometric data on the holder from the chip (column 5, lines 34-37, column 6, lines 13-16: *the fingerprint data on the chip is read and compared to the input fingerprint*);

receipt of the biometric data on the person presenting the document (column 5, lines 50-51: *user places finger on fingerprint scanner*) and comparison with the biometric data on the holder to determine whether the person presenting the document is the holder (column 5, lines 50-55: *compare input fingerprint with stored fingerprint data to determine if user is authentic*);

receipt of the holder details (column 5, lines 36-37: "identification data"), checking of the specific relationship between the holder details and the data (column 5, lines 50-55: *authenticating user*) and reading the predetermined right of the holder from the memory (column 6, lines 45-51: *wherein the user identification memory (predetermined right) is used to determine if the user is able to gain entry*);

provision of a signal to indicate the predetermined right for the person presenting the document if the chip and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder (column 7, lines 46-51), *wherein the response (signal) is sent to a gateway indicating whether access is permitted.*

Burger does not explicitly disclose that the processing unit establishes the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip and the data with the aid of a public key encryption technology. Trench discloses a system wherein a chip card contains a private key (Trench: Figure 2, item 104), which is used in a challenge along with a public key to determine if the chip card is authentic (Trench: paragraph 0026, lines 1-12). Burger and Trench are analogous arts as both use chip cards to authenticate a user. Trench uses this challenge system to assure that the chip card is authentic before letting the user proceed with a transaction (Trench: paragraph 0026, lines 10-11). This challenge-response using the private-public key technology could be used in the system of Burger after the biometric input is compared to authenticate the user. In the system of Burger, after the authentication of the user, the user identification data is read from the chip and sent to a gateway (Burger: column 6, lines 44-51). The gateway could then send a challenge to the user to verify that the chip is also authentic, as in the system of Trench, which using the method of Trench, the user can use the stored private key to respond to the challenge to verify that the chip is also authentic and allow the transaction to proceed (Trench: paragraph 0026: lines 1-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the public-private encryption method of Trench into the system of Burger so that a merchant "can be assured that the user is the legitimate certificate holder and that the user certificate belongs to the user" (Trench: paragraph 0026, lines 8-11) and so that the

merchant can "confidently accept the chip card from the user" (Trench: paragraph 0026, lines 11-12).

Burger discloses storing biometric data on a chip (Burger: column 5, lines 32-36). Trench discloses a private key which is used in challenge response to establish the authenticity of the chip (Trench: paragraph 0026, lines 10-11). The combination of Burger-Trench, therefore provides a card with a chip which stores a private key and biometric data. However, they do not teach verifying the authenticity of the data itself, but only the chip. However, Chen uses a system of using stored digital signatures to calculate a checksum, which was originally calculated using the user's information, and compares it to the stored checksum (Chen: column 9, line 55 – column 10, line 10). If the checksums (user information) do not match, then the card is rejected. The user information in this case could include the biometric information of Burger. It would have been obvious to combine Chen with the Burger-Trench combination because all three are directed towards authenticating users and chip cards.

Burger and Trench do not explicitly teach reading the machine readable holder details from a machine readable zone and checking the predetermined relationship of the data to the machine readable holder details. Chen discloses a system wherein a card stores issuer identification information (holder details) and a key which it uses to perform a one-way hash function on the user information data (Chen: column 6, lines 50-54, column 7, lines 57-63) and then the authentication unit performs its own checksum on the issuer identification number and compares the results to authenticate the user (Chen: column 7, lines 18-29). Burger discloses a key that is stored on the

card, so this key can be used to perform the hash value on the user information to create a hash, which is then compared to a hash of the results at the gateway of Burger using the process of Chen (predetermined relationship to the holder details). Burger, Trench, and Chen are analogous arts as all use chip cards for the purposes of authenticating a user. It would have been obvious to use the one-way hashing function of Chen to authenticate the user information in the system of Burger-Trench because the use of a one-way function because it "makes it impossible to work backwards to determine the checksum" (Chen: column 4, lines 9-14).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Burger discloses:

Document comprising a card provided with machine-readable holder details and a chip, which chip is provided with a processing unit and memory connected thereto and an input/output unit (column 5, lines 50-58, column 6, lines 13-18: *authentication done on board reader*), wherein the memory contains biometric data on a holder (column 5, lines 32-26: *user fingerprint information stored on chip*), as well as data that have a predetermined relationship to the holder details (column 6, lines 45-51: *wherein the user identification memory (predetermined right) is used to determine if the user is able to gain entry*), as well as instructions for making the processing unit carry out the following instructions:

transmission of the biometric data on the holder and the data from the memory to the system (column 5, lines 50-55: *compare input fingerprint with stored fingerprint data to determine if user is authentic*).

Burger does not explicitly disclose that the processing unit establishes the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip and the data with the aid of a public key encryption technology. Trench discloses a system wherein a chip card contains a private key (Trench: Figure 2, item 104), which is used in a challenge along with a public key to determine if the chip card is authentic (Trench: paragraph 0026, lines 1-12). Burger and Trench are analogous arts as both use chip cards to authenticate a user. Trench uses this challenge system to assure that the chip card is authentic before letting the user proceed with a transaction (Trench: paragraph 0026, lines 10-11). This challenge-response using the private-public key technology could be used in the system of Burger after the biometric input is compared to authenticate the user. In the system of Burger, after the authentication of the user, the user identification data is read from the chip and sent to a gateway (Burger: column 6, lines 44-51). The gateway could then send a challenge to the user to verify that the chip is also authentic, as in the system of Trench, which using the method of Trench, the user can use the stored private key to respond to the challenge to verify that the chip is also authentic and allow the transaction to proceed (Trench: paragraph 0026: lines 1-12). Therefore, it would

have been obvious to one of ordinary skill in the art at the time of invention to use the public-private encryption method of Trench into the system of Burger so that a merchant "can be assured that the user is the legitimate certificate holder and that the user certificate belongs to the user" (Trench: paragraph 0026, lines 8-11) and so that the merchant can "confidently accept the chip card from the user" (Trench: paragraph 0026, lines 11-12).

Burger discloses storing biometric data on a chip (Burger: column 5, lines 32-36). Trench discloses a private key which is used in challenge response to establish the authenticity of the chip (Trench: paragraph 0026, lines 10-11). The combination of Burger-Trench, therefore provides a card with a chip which stores a private key and biometric data. However, they do not teach verifying the authenticity of the data itself, but only the chip. However, Chen uses a system of using stored digital signatures to calculate a checksum, which was originally calculated using the user's information, and compares it to the stored checksum (Chen: column 9, line 55 – column 10, line 10). If the checksums (user information) do not match, then the card is rejected. The user information in this case could include the biometric information of Burger. It would have been obvious to combine Chen with the Burger-Trench combination because all three are directed towards authenticating users and chip cards.

Burger and Trench do not explicitly teach reading the machine readable holder details from a machine readable zone and checking the predetermined relationship of the data to the machine readable holder details. Chen discloses a system wherein a card stores issuer identification information (holder details) and a key which it uses to

perform a one-way hash function on the user information data (Chen: column 6, lines 50-54, column 7, lines 57-63) and then the authentication unit performs its own checksum on the issuer identification number and compares the results to authenticate the user (Chen: column 7, lines 18-29). Burger discloses a key that is stored on the card, so this key can be used to perform the hash value on the user information to create a hash, which is then compared to a hash of the results at the gateway of Burger using the process of Chen (predetermined relationship to the holder details). Burger, Trench, and Chen are analogous arts as all use chip cards for the purposes of authenticating a user. It would have been obvious to use the one-way hashing function of Chen to authenticate the user information in the system of Burger-Trench because the use of a one-way function because it "makes it impossible to work backwards to determine the checksum" (Chen: column 4, lines 9-14).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Burger discloses:

Document according to claim 8, wherein the document is a travel document (column 5, lines 43-46), *wherein the smart card (document) could operate as a driver's license.*

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Burger discloses:

Document according to claim 9, wherein the chip is an integral part of the travel document (column 5, lines 43-46), *wherein the smart card (document) could operate as a driver's license and is used for authenticating the holder.*

Claim 11 is rejected as applied above in rejecting claim 8. Furthermore, Burger discloses:

Document according to claim 8, wherein the input/output unit is equipped for contact-free communication (column 4, lines 65-66), *wherein the smart card can be contactless.*

Claim 12 is rejected as applied above in rejecting claim 8. Furthermore, Burger discloses:

Document according to claim 8, wherein the chip is equipped as a transponder unit (column 4, lines 65-66), *wherein the smart card can be contactless, which means that the RFID tag acts as a transponder.*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
06/19/2008
Examiner, Art Unit 2131